

Lecție 10

Structuri Algebrice în Informatică

Morfism și izomorfism de inele

I Deco $f: A_1 \rightarrow A_2$ este un morfism de inele,
notăm:

$$\ker f = \{x \in A_1 : f(x) = 0\}$$

Am văzut că $\ker f$ este ideal în A_1 .

Prop: Un morfism de inele $f: A_1 \rightarrow A_2$ este injectiv

$$\Leftrightarrow \ker f = \{0\}$$

Dtm: "Intotdeauna $0 \in \ker f$ pt că $f(0) = 0$

" \Rightarrow " P_p că f injectiv. Fie $x \in \ker f \Rightarrow f(x) = 0 = f(0) \Rightarrow$

$$\xrightarrow{1} x = 0 \Rightarrow \ker f = \{0\}$$

inv $\ker f = \{0\}$. Fie $x_1, x_2 \in A_1$ cu $f(x_1) = f(x_2)$

$\Rightarrow f(x_1) - f(x_2) = 0 \Rightarrow f(x_1 - x_2) = 0 \Rightarrow x_1 - x_2 \in \ker f = \{0\}$

$$\Rightarrow x_1 = x_2 \quad \text{decă } f \text{ injectivă. } \square$$

$$\Rightarrow x_1 = x_2$$

Teorema (Proprietatea de universalitate a inelilor de polinoame)

Fie A, R inele comutative, $f: A \rightarrow R$ morfism de inel (de ex: $A = R$ și $f = 1_A$) și $b \in R$.

Atunci există și este unic un morfism de inel $\ell: A[x] \rightarrow R$ a.p. $\ell(a) = f(a)$, ∀ $a \in A$ și

$$(ii) \quad \ell(x) = b$$

De fapt $\ell(P(x)) = P(b)$ în cazul $A = R$

$$\text{și } f = 1_A$$

avem $\ell =$ morfismul de evaluare în b .

T.F. 120 la inel

Dacă $f: A_1 \rightarrow A_2$ morfism de inel, atunci $\ker f$ ideal în A_1 și $A_1/\ker f \cong \operatorname{Im} f$ înz.
de inel

$$a \longrightarrow f(a)$$

Teorema: Fie A_1, A_2 inele comutative, I_1 ideal în A_1 și I_2 ideal în A_2 .

(1) $I_1 \times I_2$ este ideal în inelul $A_1 \times A_2$.

De fapt pentru orice ideal J în $A_1 \times A_2$ și

I_1' ideal în A_1 și I_2'' ideal în A_2 cu $J = I_1' \times I_2''$

(2) Are loc izomorfismul de inele $\frac{A_1 \times A_2}{I_1 \times I_2} \cong$

$$\frac{A_1}{I_1} \times \frac{A_2}{I_2}$$

Dem (1) Fie $(x_1, y_1), (x_2, y_2) \in I_1 \times I_2 \ni (q_1, q_2)$

$$(a'_1, a'_2) \in A_1 \times A_2$$

$$(x, y_1)(a_1, a_2) + (a'_1, a'_2)(x_2, y_2) \in I_1 \times I_2$$

$$(a_1 x_1, a_2 y_1) + (a'_1 x_2, a'_2 y_2)$$

din care

$$(a_1 x_1 + a'_1 x_2, a_2 y_1 + a'_2 y_2) \in I_1 \times I_2$$

ideale

$$(2) f(x, y) = (x, \bar{y}) = (x + I_1, y + I_2)$$

Aceasta fct. este morfism surjectiv de inele.

$$\text{Ker } f = \{(x, y) \in A_1 \times A_2 : f(x, y) = (0, \bar{0})\}$$

$$x = 0 \text{ și } \bar{y} = \bar{0} \Leftrightarrow x \in I_1, y \in I_2$$

Acum să fixăm înelele obținute.

$$A_1 \times A_2 / \text{Ker } f \cong \text{Im } f, \text{ deci } \frac{A_1 \times A_2}{I_1 \times I_2} \cong \frac{A_1 \times A_2}{I_1 \times I_2}$$

înse de inele \otimes

Ex: $A_1 = \mathbb{Z}$, $I_1 = (2) = 2\mathbb{Z}$ idealul generat de 2, respectiv 3.
 $A_2 = \mathbb{Z}$, $I_2 = (3) = 3\mathbb{Z}$

Astunci $\frac{\mathbb{Z} \times \mathbb{Z}}{2\mathbb{Z} \times 3\mathbb{Z}} = \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}} = \mathbb{Z}_2 \times \mathbb{Z}_3$ este de sine

(este un mulțim 6 el.)

$$\cong \mathbb{Z}_6$$

Def Fie I_1, I_2 ideale în mulțimea A . Astunci

multimea $I_1 + I_2 = \{x + y : x \in I_1, y \in I_2\}$

este un ideal în A numit suma idealor I_1, I_2

Dacă $x_1 + y_1 \in I_1 + I_2$ cu $x_1 \in I_1$ și $y_1 \in I_2$

$x_2 + y_2 \in I_1 + I_2$ cu $x_2 \in I_1$ și $y_2 \in I_2$

$a, b \in A$

$$a(x_1 + y_1) + b(x_2 + y_2) = (ax_1 + bx_2) + (ay_1 + by_2)$$

$$a \in I_1 \quad b \in I_2$$

$\in I_1 + I_2$

Dacă $I_1 + I_2$ este un ideal în A .

Obs! $I_1 + I_2$ este idealul generat de $I_1 \cup I_2$

în general $I_1 \cup I_2$ este ideal ($\Leftrightarrow I_1 \subseteq I_2$ sau inclus)

$I_1 \supseteq I_2$

(inclus)

Dcf două ideale $I_1 \neq I_2$ din inelul \mathbb{Z} și α numește COMAXIMALE dacă $I_1 + I_2 = \mathbb{Z}$

Ex: $\exists m \in \mathbb{Z}$, $I_1 = (m) = m\mathbb{Z}$, $I_2 = (n) = n\mathbb{Z}$

$$I_1 + I_2 = \{m \cdot k + n \cdot l \mid k, l \in \mathbb{Z}\} = (m, n) = (\gcd(m, n))\mathbb{Z}$$

Afunci I_1, I_2 sunt ideale comaximale
în \mathbb{Z}

$$\Leftrightarrow \gcd(m, n) = 1$$

De exemplu dacă p_1, p_2 prime distincte \Rightarrow

$\Rightarrow (p_1^{\alpha_1}) \neq (p_2^{\alpha_2})$ sunt ideale comaximale
în \mathbb{Z} și $\gcd(p_1^{\alpha_1}, p_2^{\alpha_2}) = 1$.

Ex: Inelul $K[X]$ cu K corp ($\mathbb{Q}, \mathbb{R}, \mathbb{C}$)

și idealul principal

$$I_1 = (f) \quad I_2 = (g) \quad \text{cu } f, g \in K[X]$$

$$I_1 + I_2 = \{f \cdot u + g \cdot v \mid u, v \in K[X]\}$$

$$= (f \cdot g) = (\gcd(f, g))K[X]$$

$I_1 = (f) \neq I_2 = (g)$ sunt ideale comaximale

$$\text{în } K[X] \Leftrightarrow \gcd(f, g) = 1.$$

f, g prime între ele

lema chineză a resturilor (LCM)

Teorema: Fie A inel comutativ și I_1, I_2, \dots, I_n ideale comaximale și cotele i radici $I_i + I_j = A$,
 $(m \in A)$
 $\forall i \neq j \leq n$.

Atunci sunt loc 120 de inele $\frac{A}{I_1 \cap I_2 \cap \dots \cap I_m} \cong$

$$A/I_1 \times A/I_2 \times \dots \times A/I_m$$

$$\xrightarrow{x} (x + I_1, x + I_2, \dots, x + I_m)$$

Aplicații

(1) $A \in \mathbb{Z}$ cu $I_1 = (m)$ și $I_2 = (n)$ ideale comaximale, adică $(m, m) = \mathbb{Z} \Leftrightarrow \gcd(m, m) = 1$.

Atunci $\frac{\mathbb{Z}(m) \cap (n)}{(m) \cap (n)} \cong \mathbb{Z}/(m) \times \mathbb{Z}/(n)$

$$(m) \cap (n) = (\text{lcm}(m, n)) = (m \cdot n)$$

$\mathbb{Z}_{m \cdot n} \cong \mathbb{Z}_m \times \mathbb{Z}_n$, $\forall m, n$ cu $\gcd(m, n) = 1$.

LCM pentru \mathbb{Z}

Ex: $\gcd(2, 3) = 1 \Rightarrow \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$ 120 de condiții $\gcd(m, n) = 1$ pt LCM este existătoare.

$\mathbb{Z}_2 \times \mathbb{Z}_2 \not\cong \mathbb{Z}_4$ (nu sunt inele izomorfe)

② În \mathbb{Z} . Fix p_1, p_2, \dots, p_t prime distincte
 $\alpha_1, \alpha_2, \dots, \alpha_t$ și
Atunci notăm $x = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_t^{\alpha_t}$

$$\frac{\mathbb{Z}}{p_1^{\alpha_1}}$$

Atunci $\mathbb{Z}_N \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_t^{\alpha_t}}$
*

izo de inele

~~Notație~~ folosim LCM astăzi $I_\ell = (p_\ell^{\alpha_\ell})$ ideal
în \mathbb{Z} pt $\ell = 1, t$

I_1, I_2, \dots, I_t sunt ideale comaximale
2 cote 2

Consequently am izomorfismul $\xrightarrow{*}$

$\Rightarrow \mathbb{Z}_N \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_t^{\alpha_t}}$ au același
nr. de elemente

$|U(\mathbb{Z}_N)| = |\{x \in \mathbb{Z}_N : \gcd(x, N) = 1\}| =$

$= \varphi(N)$ funcție indicatoare a lui Euler

$$|U(\mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_t^{\alpha_t}})| = |U(\mathbb{Z}_{p_1^{\alpha_1}}) \times U(\mathbb{Z}_{p_2^{\alpha_2}}) \times \cdots \times U(\mathbb{Z}_{p_t^{\alpha_t}})|$$

$$= \prod_{i=1}^t |U(\mathbb{Z}_{p_i^{\alpha_i}})| = \prod_{i=1}^t \varphi(p_i^{\alpha_i})$$

$$\varphi(p_i^{\alpha_i}) = |\{x \in \mathbb{Z} : 0 \leq x \leq p_i^{\alpha_i}, \gcd(x, p_i^{\alpha_i}) = 1\}|$$

$$\gcd(x, p_i^{\alpha_i}) = 1, \quad p_i \nmid x$$

$$\xrightarrow{p_i^{\alpha_i}} = p_i^{\alpha_i} - |\{x \in \mathbb{Z} : 0 \leq x < p_i^{\alpha_i}, p_i \mid x\}|$$

$$= p_i^{d_i} - \left| \{0, p_i, 2p_i, \dots, p_i^{d_i-1}\} \right| =$$

$$= p_i^{d_i} - p_i^{d_i-1} = p_i^{d_i} \left(1 - \frac{1}{p_i}\right)$$

Deci $\ell(x) = \pi_{p_i}^{d_i} \left(1 - \frac{1}{p_i}\right) = x \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_t}\right)$
 $\forall x \in \mathbb{N}^*, x \geq 2$

$\ell(1) = 1$ prin definitie

(B) Fie $m, m_1, \dots, m_t \in \mathbb{N}^*$ prime între ele 2 către 2
 ca și $\gcd(m_i, m_j) = 1, \forall i \neq j \leq t$

Fie $a_1, a_2, \dots, a_t \in \mathbb{Z}$. Atunci sistemul de congruențe are o unică soluție $x = m_1 \cdot m_2 \cdots m_t (x_0)$

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_t \pmod{m_t} \end{cases} \quad (\exists ! x_0 \in \{0, 1, 2, \dots, N-1\})$$

Deși soluțiile sunt $S = \{x_0 + k \cdot x : k \in \mathbb{Z}\}$

Avem: $\text{LCM}(\mathbb{Z}_N) \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_t}$
 îzo să imul

$$x \longrightarrow (x \pmod{m_1}, x \pmod{m_2}, \dots, x \pmod{m_t})$$

Ex: rezolvare în \mathbb{Z} : $\begin{cases} x \equiv 1 \pmod{15} \\ x \equiv 5 \pmod{8} \end{cases}$

$$15 = m_1$$

$$1 = q_1$$

$$8 = m_2$$

$$5 = q_2$$

$$\gcd(15, 8) = 1$$

$$N = 15 \cdot 8 = 120$$

$$f = \{ b + k \cdot 120 \mid k \in \mathbb{Z} \}$$

$$\exists ! x_0 \text{ soluție mod } 120 \Rightarrow f = \{ 61 + k \cdot 120 \mid k \in \mathbb{Z} \}$$

$$= 61$$

~~(A) $K[x]$ cu f, g polinoame cu $\gcd(f, g) = 1$~~

~~(B) $K[x]$ cu f, g polinoame cu $\gcd(f, g) = 1$~~

$$A \subset \text{Atunci } \frac{\text{lcm}}{(f, g)} \sim \frac{K[x]}{(f)} \times \frac{K[x]}{(g)}$$

izo de inele

Corpuzi

Când un mul factor este corp?

$\mathbb{Z}/(m) \cong \mathbb{Z}_m$ este corp $\Leftrightarrow m$ este nr. prim

Prop: Fix $f \in K[x]$ cu K corp. Atunci:

$K[x]/(f)$ este corp $\Leftrightarrow f$ este polinom irreductibil în $K[x]$

Dacă „ \Rightarrow ” pp. $K[x]/(f)$ corp $\Rightarrow \hat{0} \neq \hat{1} \Rightarrow$

$\Rightarrow (f) \neq K[x] \Rightarrow f$ neconstant

decă B.A. $f = g_1 \cdot g_2$ cu $g_1, g_2 \in K[x]$ neconstante

$$0 < \underbrace{\text{grad } g_1, g_2}_{\text{grad } f} < \text{grad } f$$

$$\text{în } K[x]/(f) \quad \hat{p} = \hat{g}_1 \cdot \hat{g}_2$$

$$\hat{0} = \hat{g}_1 \cdot \hat{g}_2 \Rightarrow \hat{g}_1 = \hat{0} \text{ sau } \hat{g}_2 = \hat{0}$$

$\Rightarrow f/g$, sau f/g_2 continuare

$\text{grad } g_1, \text{grad } g_2 < \text{grad } f$

$n \in \mathbb{N}$ fix $\hat{g} + \delta \in K[x]/(f)$. Arăt că \hat{g}^{-1} este inversabilă

$g \notin (f) \Leftrightarrow f \nmid g \Leftrightarrow \text{gcd}(f, g) = 1 \xrightarrow{\text{euclidian}}$

$\exists u, v \in K[x]$ cu $u \cdot f + v \cdot g = 1$

$\text{mod } f \Rightarrow \bar{v} \cdot \hat{g} = 1 \in K[x]/(f) \Rightarrow \hat{g}$ este inversabilă
în $K[x]/(f)$ $\Rightarrow K[x]$ este corp

(K1) Ex: $f(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$

este ireducibil în $\mathbb{Z}_2[x]$

$\mathbb{Z}_2[x]/(x^3 + x + 1)$ este corp. $= \{ \overline{a + bx + cx^2} : a, b, c \in \mathbb{Z}_2 \}$

\hookrightarrow corp cu 8 elemente

(K2) Alt ex: Analog $\mathbb{Z}_2[x]/(x^3 + x^2 + 1)$ corp cu 8 elemente
izomorf cu K1.